Denial of Service (DoS) Vulnerability in MELSEC iQ-R Series Ethernet Interface Module

Release date: November 29, 2022
Last update date: December 6, 2022
Mitsubishi Electric Corporation

■Overview

Denial of Service (DoS) Vulnerability exists in MELSEC iQ-R Ethernet Interface Module. This vulnerability allows a remote unauthenticated attacker to cause a Denial of Service (DoS) condition on a target product by sending specially crafted packets.(CVE-2022-40265)

The model names and firmware versions affected by this vulnerability are listed below. Please take the following Countermeasures or Mitigations/Workarounds.

■CVSS[1]

CVE-2022-40265 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H Base Score:8.6

■Affected products

Affected products and versions are below.

Series	Product Name	Version
MELSEC iQ-R Series	RJ71EN71	Firmware version "65" and prior
	R04/08/16/32/120ENCPU (Network Part)	Network Part Firmware version "65" and prior

Please refer to the following manual for how to check the firmware version.
- MELSEC iQ-R Module Configuration Manual "Appendix 1 Checking Production Information and Firmware Version"

Please download the manual from the following URL.
https://www.mitsubishielectric.com/fa/download/index.html

■Description

Denial of Service (DoS) Vulnerability due to Improper Input Validation(CWE-20)[2] exists in MELSEC iQ-R Series Ethernet Interface Module.

■Impact

A remote unauthenticated attacker may cause a DoS condition on a target product by sending specially crafted packets. A system reset is required for recovery from a Denial of Service (DoS) condition.

■Countermeasures

We have fixed the vulnerability at the following version.

Series	Product Name	Version
MELSEC iQ-R Series	RJ71EN71	Firmware version "66" or later
	R04/08/16/32/120ENCPU (Network Part)	Network Part Firmware version "66" or later

Please download fixed firmware update file from the following site and update the firmware.
https://www.mitsubishielectric.com/fa/download/index.html

Please refer to the following product manual for how to update firmware.
- MELSEC iQ-R Module Configuration Manual "Firmware Update Function"

■Mitigations/Workarounds

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:

- Use a firewall, virtual private network (VPN), etc. to prevent unauthorized access when Internet access is required.
- Use within a LAN and block access from untrusted networks and hosts through firewalls.
- Use the IP filter function*1 to restrict the accessible IP addresses.

*1 : MELSEC iQ-R Ethernet User's Manual(Application) Security "IP filter"

■Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries | MITSUBISHI ELECTRIC FA>
https://www.mitsubishielectric.com/fa/support/index.html

1 https://www.first.org/cvss/v3.1/specification-document
2 https://cwe.mitre.org/data/definitions/20.html

■Update history
December 6, 2022
Corrected clerical errors of URL of “Affected products” and “Countermeasures”.